# 技術情報:Si-R/Si-R brinシリーズ設定例

「Windows Azure」との接続(ルートベースIPsec)

Si-R Gシリーズで「Windows Azure」ルートベースIPsec接続する場合の設定例です。

[対象機種と版数] Si-R Gシリーズ V2.16以降、V3.02以降

[設定内容]

- ・Si-R Gのether 1 1をWAN側、ether 2 1-4をLAN側とします。
- ・WAN側は、PPPoEで固定グローバルアドレスが1つ割り当てられるとします。
- ·Si-RLAN側に192.168.1.1/24を割り当てるとします。
- ・Azure側では、10.0.0.0/8の仮想ネットワークの中に、
- ゲートウェイサブネット10.1.0.0/24が存在するとします。
- ・IPv4 over IPv4 IPsec tunnelで拠点間を接続します。



オンプレミス側ネットワーク

項目	環境情報
接続メディア	FTTHなど
接続プロトコル	PPPoE
WAN	固定グローバルアドレス
LAN	192.168.1.0/24

オンプレミス側ネットワークでは、Si-RでPPPoE(アドレス固定)を行います。 固定のアドレスを使用して、Azureネットワークに対して、IPsec接続を動作させます。

## Windows Azure側ネットワーク

Windows azure 仮想ネットワークでは、10.0.0.0/8のアドレス空間の中に、1つのサブネット が存在します。

サブネット名	アドレス範囲
Gateway subnet	10.1.1.0/24

オンプレミス側とWindows Azure側でのIPsecにより、IPsecトンネルを介して、オンプレミスからAzure側のサブネットに対して通信をすることが可能となります。

## **Windows Azure**での設定

本章ではオンプレミス側とのIPsec接続をするためのAzureでの設定について説明します。

## リソースグループの作成

Windows Azure ポータルサイトにログインし、[リソースグループ]-[追加]の順に選択します。

Microsoft Azure 🗸	リソース グループ		₽ リンースの検索	× 🗘 🖉 🖉	0 😳	展進のディレクトリ
=	101 7 64 7					
+ 55.0	リソースクループ 既定のデルクトリ					
🎯 リソース グループ	+ Ⅲ ひ 追加 列 更新					
ⅲ すべてのリソース	サブスクリプション: 無料試用版					
🕒 最近使った項目	マイルター項目。					
🔕 App Service	名前	サブスクリプション		18/99		
🧕 仮想マシン (クラシック)						
Virtual Machines						
🗟 SQLデータペース						
Cloud Services (クラシー・						
🏮 セキュリティ センター						
📍 サブスクリプション						
参照 >						
https://portal.azure.com						

[リソースグループ名],[リソースグループの場所]を入力、または選択し、[作成]を選択し ます。

Microsoft Azure 🗸	リソース グループ > リソース グループ	P リソースの検索	× 🖓 🖉 😳 🕜 📖	, 🕘
=	_			
+ ###	シリース クループの作成			
🞯 リソース グループ				
ⅲ すべてのリソース	* リソース グループ名			
昼近使った項目	IPsec 🗸			
App Service	* サブスクリプション 無料認用版			
👰 仮想マシン (クラシック)	* リソース グループの場所			
👰 Virtual Machines	東日本			
👼 SQLデータペース				
🐠 Cloud Services (クラシー・				
🔋 セキュリティ センター				
💡 サブスクリプション				
参照 >				
	ダッシュボードにピン留めする			
	作成			
	X.J.			

設定内容	設定値
リソースグループ名	IPsec
リソースグループの場所	東日本

## 仮想ネットワークの作成

Windows Azureポータルサイトから、[新規]-[ネットワーキング]-[Virtual Network]の順に選択します。



## [デプロイモデルの選択]でリソースマネージャーを選択し、[作成]を選択します。

Microsoft Azure 👻	新規 > ネットワーキング > Vir	tual Network	₽ リソースの被素	× 🖓 / 🏟 🙄 O	เปลา เปลา 🥹
三 + 新規	Virtual I Microsoft	* _ 🗆 ×			
	COP+1/7-2/9-1/2 装飾し、 細枝を表用して、このたりシンとオ キャリークを支持など、EMA(4) ・シンへの細枝を凝集するとど、 低整キャリークを利用すると、 低整キャリークを利用すると、 の モージンク・の現象 ・ ジングンク・シンクの用・ ・ ・ ジングンク・シンクの用・ ・ 、 ・ 、 ・ 、 、 、 、 、 、 、 、 、 、 、 、 、	: 論理的いう確認さたなりからる Microsoft Auris に 石成()ます: Italie フルンステークビンターをたら 1 6005(アント マンスに開せてきます。 彼徳 第4) Aurie (クンス) サジヤ セスアンドで (管理に必用したな) あい Unix (学校ではなンタンと思め、ポンプレンスのデータをよびアブリン ます。 ことが自然にかます。 Microsoft			
<ul> <li>● セキルディセンター・</li> <li>              ◆ サガスのはひっよ             ◆             新二</li></ul>	<u>ፀድወ</u> ታውን	1年130月 サービスの展開 現在できなりスートコン 料金の開始			
	デプロイモデルの単尺 ● リソース マネージャー の政	×			

設定内容	設定値
デプロイモデルの選択	リソースマネージャー

仮想ネットワークの作成の設定項目が表示されます。 仮想ネットワークの作成で[名前],[アドレス空間],[サブネット名],[サブネットアドレス範 囲],[リソースグループ],[場所]を入力、または選択し、[作成]をクリックします。

Microsoft Azure 🗸	新規 > ネットワーキング > Virtual Network > 仮	想ネットワークの作成	)リゾースの従素	< 🗘 🖉 😳 O	REDFALOHI
=	_ ロ × 仮想ネットワークの作成				
十新規					
📦 リソース グループ					
オペてのリソース	* 名前				
④ 最近使った項目	AzureNet ✓				
App Service	10.1.0.0/16				
👰 仮想マシン (クラシック)	* サブネット名				
Virtual Machines	* サブネット アドレス範囲 ●				
■ SQLデータペース	10.1.0.0/24 10.1.0.0 - 10.1.0.255 (256 FFVX)				
Cloud Services (クラシー	<ul> <li>* サブスクリプション</li> <li>無料試用版</li> </ul>				
	* リソース グループ ●				
	◎ 新規 ⑧ Use existing				
	* 場所				
	★日東				
	□ ダッシュホードにビン留めする				
	find days				

設定内容	設定値
名前	AzureNet
アドレス空間	10.1.0.0/16
サブネット名	default
サブネットアドレス範囲	10.1.0.0/24
リソースグループ	IPsec
場所	東日本

以上で仮想ネットワークの作成が完了します。

## 仮想ネットワークゲートウェイの作成

次に、VPNを張るためのゲートウェイを作成します。

Windows Azureポータルサイトから、[新規]-[ネットワーキング]-[仮想ネットワークゲートウェイ]の順に選択します。



#### 仮想ネットワークゲートウェイの作成の設定項目が表示されます。 [名前],[仮想ネットワーク],[ゲートウェイサブネットのアドレス範囲],[パブリックIPアドレ ス],[ゲートウェイの種類],[VPNの種類],[場所]を選択、または入力します。



設定内容	設定値
名前	AzureGW
仮想ネットワーク	AzureNet
ゲートウェイサブネットのアドレス範囲	10.1.1.0/24
パブリックIPアドレス	(新規)AzureGW
ゲートウェイの種類	VPN
VPNの種類	ルートベース
場所	東日本

以上で仮想ネットワークゲートウェイの設定が完了します。

## ローカルネットワークゲートウェイの作成

Azure側でオンプレミス側の情報を設定します。

Windows Azureポータルサイトから、[新規]-[ネットワーキング]-[ローカルネットワークゲートウェイ]の順に選択します。



ローカルネットワークゲートウェイの作成の設定項目が表示されます。 オンプレミス側の情報を、[名前],[IPアドレス],[アドレス空間],[リソースグループ],[場所]に入 カ、または選択します。

Microsoft Azure 🗸	新規 > ネットワーキング > ローカル ネットワーク ゲートウ	イの作成	P リソースの検索	× 🗘 🖉 😳 📀	<b>歴定のディレクトリ</b>
	_ □ × □−カル ネットワーク ゲートウェイの…				
十新規					
🚳 リソース グループ					
🏭 すべてのリソース	* 2m				
④ 最近使った項目	si-R 🗸				
🔇 App Service	XXX.XXX.XXX V				
🧕 仮想マシン (クラシック)	7下レス空間 0				
👰 Virtual Machines	192.168.1.0/24				
🗟 SQL データペース	その他のアドレス範囲の追加				
🧼 Cloud Services (クラシー	* サブスクリプション 無利利式用版				
🯮 セキュリティ センター	* リソース ヴループ ロ				
↑ サブスクリプション	Psed				
参照 >	* 坦斯				
	東日本 🗸				
	□ ダッシュホードにどう編めする				
	作成 c <sup>lin</sup> y				

設定内容	設定値
名前	Si-R
IPアドレス	XXX.XXX.XXX.XXX
アドレス空間	192.168.1.0/24
リソースグループ	IPsec
場所	東日本

以上でローカルネットワークゲートウェイの作成が完了します。

## 接続の作成

ここまでで作成した、仮想ネットワークゲートウェイと、ローカルネットワークゲートウェ イを接続により結び付け、IPsecの接続を行います。

Windows Azureポータルサイトから、[新規]-[ネットワーキング]-[すべて表示]の順に選択します。





接続の作成が表示されます。1.基本、2.設定、3.概要についてそれぞれ設定を行います。 [基本]を選択し、基本の設定を行います。[接続の種類],[リソースグループ],[場所]をそれぞれ選択し、[OK]をクリックします。



設定内容	設定値
接続の種類	サイト対サイト(IPsec)
リソースグループ	IPsec
場所	東日本

2.設定が表示されます。[仮想ネットワークゲートウェイ],[ローカルネットワークゲート ウェイ],[接続名],[共有キー]を選択、または入力し、[OK]をクリックします。

Microsoft Azure 🐱	《 接続の作成 〉 設定		<b>り</b> リソースの検索	× 🗳 🖉	© 0	
=	_ = ×	_ = >	<			
十新現	接続の作成	設定				
😭 101-7 di -7						
			•			
······································	1 8*	* 仮想ネットワーク ゲートウェイ 0				
昼 最近使った項目	▲ ●◆設定を構成していたい	AzureGW				
App Service		* ローカル ネットワーク ゲートウェイ O Si-R				
👰 仮想マシン (クラシック)	∠ 接続設定を構成してくたさい >	51.14				
Virtual Machines		* 理研究 AzureGW-Si-R				
🗟 SQL データペース	3 根長 >	* ###±- (PSK) @				
Cloud Services (クラシー・		test 🗸				
a tetralization						
7 サフスクリプション						
参照 >						
			_			
		OK				

設定内容	設定値
仮想ネットワークゲートウェイ	AzureGW
ローカルネットワークゲートウェイ	Si-R
接続名	AzureGW-Si-R
共有キー	test

接続の作成で設定した項目の確認画面が表示されます。設定内容を確認し、[OK]をクリックします。



以上でAzure側での設定は完了です。

オンプレミス(Si-R)での設定 本章では、Windows AzureとIPsec接続するためのSi-Rの設定について解説します。

## IPsec設定項目

IPsec設定値については、以下のような内容になります。 IKEフェーズ1

項目	設定値
IPsec情報のセキュリティプロトコル	esp
暗号情報	aes-cbc-256
認証(ハッシュ)情報	hmac-sha1
IPsec SA 有効時間	2h
DHグループ	off
ESN(拡張シーケンス番号)	disable
IPsec対象範囲(送信元)	192.168.1.0/24
IPsec対象範囲(宛先)	10.0.0/8

## IKEフェーズ2

項目	設定値
自側トンネルエンドポイントアドレス	192.168.1.1
相手側トンネルエンドポイントアドレス	ууу.ууу.ууу.ууу
	ポータルサイトより確認
lan側ローカルアドレス	192.168.1.1/24
暗号情報	aes-cbc-256
認証(ハッシュ)情報	hmac-sha1
DHグループ	group 2(modp1024)
PRF(疑似乱数関数)	hmac-sha1
IKE SA有効時間	2h
NAT-TRAVERSAL	on
IKEセッション共有鍵	ポータルサイトに設定した値を使用

## 相手側トンネルエンドポイントアドレスの確認

ポータルサイトより、[リソースグループ]を選択し、対象のリソースグループ、接続をクリックします。 接続に表示された[仮想ネットワークゲートウェイ]が、相手側エンドポイントアドレスとなり



#### config

configの全体像としては以下のような内容になります。 configは大きく分けて、etherポート定義、lan定義、PPPoE定義、IPsec定義に分けられます。 それぞれについて順を追って説明していきます。

ether 1 1 vlan untag 1 ether 2 1-4 vlan untag 2 lan 1 ip address 192.168.1.1/24 3 lan 1 vlan 2 remote 0 name PPPoE remote 0 mtu 1454 remote 0 ap 0 name PPPoE remote 0 ap 0 datalink bind vlan 1 remote 0 ap 0 ppp auth send id@isp pass@isp remote 0 ap 0 keep connect remote 0 ppp ipcp vicomp disable remote 0 ip route 0 default 1 1 remote 0 ip nat mode multi any 1 5m remote 0 ip nat wellknown 0 500 off remote 0 ip msschange 1414 remote 1 name Azure remote 1 ap 0 name IPSec remote 1 ap 0 datalink type ipsec remote 1 ap 0 keep connect remote 1 ap 0 ipsec type ikev2 remote 1 ap 0 ipsec ike protocol esp remote 1 ap 0 ipsec ike range 192.168.1.0/24 10.0.0.0/8 remote 1 ap 0 ipsec ike encrypt aes-cbc-256 remote 1 ap 0 ipsec ike auth hmac-sha1 remote 1 ap 0 ipsec ike lifetime 2h remote 1 ap 0 ipsec ike esn disable remote 1 ap 0 ike local-idtype address remote 1 ap 0 ike remote-idtype address remote 1 ap 0 ike shared key text test remote 1 ap 0 ike proposal 0 encrypt aes-cbc-256 remote 1 ap 0 ike proposal 0 hash hmac-sha1 remote 1 ap 0 ike proposal 0 lifetime 2h remote 1 ap 0 ike proposal 0 pfs modp1024 remote 1 ap 0 ike proposal 0 prf hmac-sha1 remote 1 ap 0 ike nat-traversal use on remote 1 ap 0 ike dpd use on remote 1 ap 0 tunnel local 192.168.1.1 remote 1 ap 0 tunnel remote yyy.yyy.yyy remote 1 ip route 0 10.0.0/8 1 1 remote 1 ip msschange 1350

#### etherポートの設定

各etherポートにVLAN(untag)を割り当てます。これは、後のlan定義や、PPPoEの定義と結びつきます。

ether 1 1 vlan untag 1 ether 2 1-4 vlan untag 2

wan側のポートに対してvlan 1を、lan側のポートに対してvlan 2を設定します。

#### PPPoEの設定

WAN側にPPPoEの設定をします。PPPoEの送出先としてvlan 1(ether 1 1)を指定します。

remote 0 name PPPoE remote 0 mtu 1454 remote 0 ap 0 name PPPoE remote 0 ap 0 datalink bind vlan 1 remote 0 ap 0 ppp auth send id@isp pass@isp remote 0 ap 0 keep connect remote 0 ppp ipcp vjcomp disable remote 0 ip msschange 1414

項目	設定値
ID(PPPoE)	id@isp
PASS(PPPoE)	pass@isp

mtu値、mss値については回線により異なります。回線側にご確認ください。

remote 0 ip route 0 default 1 1

PPPoEのインタフェースに対してデフォルトルートを設定します。

remote 0 ip nat mode multi any 1 5m remote 0 ip nat wellknown 500 off

mode multiの設定により、NAPTの設定が有効になります。nat wellknownの定義により、 ISAKMP(UDP/500)に対してポート変換を行います。 Si-RからのNAT-Traversalを使用したIPsec接続が可能となります。

#### Ian側アドレスの設定

lan側のアドレスを192.168.1.1/24に設定します。このlanインタフェースはvlan 2の物理 ポートと結びつきます。

lan 1 ip address 192.168.1.1/24 3 lan 1 vlan 2

#### **IPsec**の設定

まず、設定するインタフェースをIPsecができるようにするため、インタフェースの転送 方式、IPsecタイプを設定します。

remote 1 ap 0 datalink type ipsec remote 1 ap 0 ipsec type ikev2 remote 1 ap 0 ike proposal 0 encrypt aes-cbc-256 remote 1 ap 0 ike proposal 0 hash hmac-sha1 remote 1 ap 0 ike proposal 0 pfs modp1024 remote 1 ap 0 ike proposal 0 pf hmac-sha1 remote 1 ap 0 ike proposal 0 lifetime 2h remote 1 ap 0 ike nat-traversal use on remote 1 ap 0 ike dpd use on remote 1 ap 0 tunnel local 192.168.1.1 remote 1 ap 0 tunnel remote yyy.yyy.yyy.

事前共有鍵(ike shared key)、相手側トンネルエンドポイント(tunnel remote)については、 Windows Azureポータルサイトにて確認した内容を設定します。 lifetimeは、Azure側の値を超えないように設定してください。 ※自側トンネルエンドポイント(tunnel local)にLAN側のアドレスを設定していますが、 NATされグローバルアドレスxxx.xxx.xxxとなりますので問題はありません。

**IKEフェーズ2** <u>IPsec設定項目</u>:IKEフェーズ2表にて提示した内容を設定します。

remote 1 ap 0 ipsec ike protocol esp remote 1 ap 0 ipsec ike range 192.168.1.0/24 10.0.0.0/8 remote 1 ap 0 ipsec ike encrypt aes-cbc-256 remote 1 ap 0 ipsec ike auth hmac-sha1 remote 1 ap 0 ike proposal 0 lifetime 2h remote 1 ap 0 ipsec ike esn disable

ike range設定の対向側のセグメントについては注意が必要です。ゲートウェイサブネットではなく、仮想ネットワークのセグメントを設定してください。 lifetimeは、Azure側の値を超えないように設定してください。 ※2014年11月より強制トンネリングが使用可能となりました。強制トンネリングを使用 する場合は、次を参照してください。<u>強制トンネリングについて</u>

## その他

ルート設定、MSS値の設定をします。このMSS値はカプセル化の方式によって変わります。今回は1350を設定します。

remote 1 ip route 0 10.0.0/8 1 1 remote 1 ip msschange 1350

以上で設定が完了です。 最後に設定をsaveして再起動します。

save

reset

## IPsec確立確認方法

ポータルサイトより、[リソースグループ]を選択し、対象のリソースグループ、接続をクリックします。接続の状態が[接続済み]となっていれば、IPsec接続が完了しています。

Microsoft Azure 🗸	リソースグループ 〉 IPsec 〉 AzureGW-Si-R 〉 證	Ê	P 11-2	の検索	× 🗘 🖉 😂 😳	💿 🔜 🔊
	* _ □ × リンノース グループ	( IPsec			AzureGW-Si-R	* _ =
十新規	臣定のディレクトリ	₩ <b>1</b> 117-2 Ø14-3			*** ##	
🞯 リソース グループ		수 + 0 고운 2010 HMR	O 更新		202 NIB	
₩ すべてのリソース	サブスクリプション: 無料試用板	要点 へ		A 12	⊘ 要点 ^	A 19
④ 最近使った項目	フィルター項目。	サブスクリプション名	サブスクリプション ID c9b8af70-613	e-4fd2-afef-f50132d477	リソース グループ	データ入力 236.04 KB
🔇 App Service	名前	前回のデプロイ 2016/6/7(成功)	場所 東日本		状態 接続済み	データ出力 187.1 KB
👰 仮想マシン (クラシック)	(🐑 IPsec 🚥			すべての設定	€→ 東日本	仮想ネットワーク AzureNet
💻 Virtual Machines		极要			サブスクリプション名 無料試用版	伝想ネットワーク ゲートウェイ AzureGW (ソソ・ソソ・ソソ・ソソ)
🥫 SQLデータペース		フィルター項目。			サブスクリプション ID c9b8af70-613e-4fd2-afef-f50132d477-	ローカル ネットワーク ゲートウェイ Si-R (xox xox xox xox xox)
🧼 Cloud Services (クラシー		6N	種類 リンースグループ	7 嶋所 サブク	00	すべての他の
🔋 セキュリティ センター		🔯 Ubuntu	仮想マシン IPsec	東日本 無料	試冊	
💡 サブスクリプション		<> AzureGW-Si-R	报纸 IPsec	東日本 無料	<b>1</b> 戊円	
810 >		<> Si-R	ローカルネ., IPsec	夏日本 無料	試用	
		ubuntu746	ネットワー IPsec	夏日本 無料	<b>試用</b>	
		Ubuntu	ネットワー IPsec	東日本 無料	ば用	
		AzureGW	パブリック L. IPsec	東日本 無料		
		Ubuntu	ADUST L. IPsec	東日本 無料	5049. ••• 103	
		() AzureOw	仮想ネット. IPsec	東口本 熱料	p.19	N
		ipsec1874	ストレージ IPsec	夏日本 無料	3012	ω.
		ipsec3944	ストレージ IPsec	夏日本 無料	試用	
		4 1			•	

Si-Rを接続し、少し時間がたってからshow access-pointコマンドを実行して確認してください。 正常にIPsecが確立できていれば下記のような結果が得られます。

#show access-point
remote 1 ap 0 : Azure.IPSec
status : connected
since : Jun 7 22:54:55 2016
speed : not available
send traffic : not available
receive traffic : not available
type : IPsec/IKE
IKE Version : 2
IKE SA : established
IPsec SA : established

IKE SA,IPsec SAともにestablished、status connectedとなっていれば接続ができています。

## 強制トンネリングについて

2014年11月より、強制トンネリングが使用可能となりました。強制トンネリングでは、仮想 ネットワークからインターネットにバインドされたトラフィックがすべてオンプレミスの場所 にリダイレクトまたは『強制的に』戻されます。

本章では、強制トンネリングの設定について解説します。

#### オンプレミス(Si-R)での設定

基本的には、強制トンネリングを使用しない設定とほとんど同じです。異なる点は、Si-Rでの range設定のみです。

下記のように設定を変更してください。

本設定変更により、オンプレミス側のIPsec化対象範囲が192.168.1.0/24から0.0.0.0/0に変更にな ります。

強制トンネリングを使用しない場合

remote 1 ap 0 ipsec ike range 192.168.1.0/24 10.0.0.0/8



強制トンネリングを使用する場合

remote 1 ap 0 ipsec ike range any4 10.0.0.0/8

#### Windows Azureでの設定

Azure側では、インターネットへの通信をオンプレミス経由で行う必要があります。そこで、 ルーティングテーブルなどの設定が必要となります。 設定についてはAzureの資料をご確認ください。